Apress®

区块链

基础知识25讲

Blockchain Basics

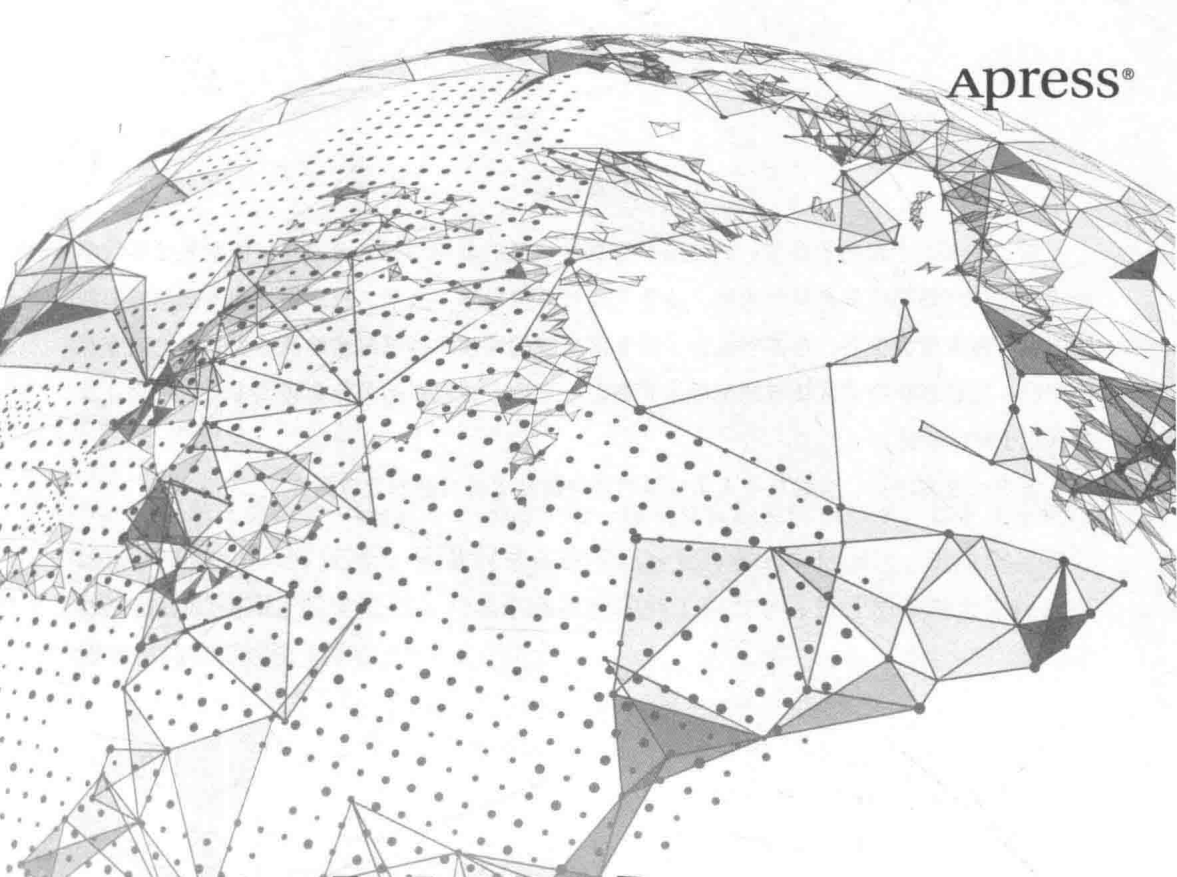
A Non-Technical Introduction in 25 Steps

[英] 丹尼尔·德雷舍（Daniel Drescher） 著

马丹 王扶桑 张初阳 译

中国工信出版集团

人民邮电出版社
POSTS & TELECOM PRESS



Apress®

区块链

基础知识 25 讲

Blockchain Basics

A Non-Technical Introduction in 25 Steps

[英] 丹尼尔 · 德雷舍（Daniel Drescher） 著

马丹 王扶桑 张初阳 译

人 民 邮 电 出 版 社

北 京

图书在版编目（CIP）数据

区块链基础知识25讲 / （英）丹尼尔·德雷舍（Daniel Drescher）著 ; 马丹, 王扶桑, 张初阳译. -- 北京 : 人民邮电出版社, 2018.11
ISBN 978-7-115-49406-1

Ⅰ. ①区… Ⅱ. ①丹… ②马… ③王… ④张… Ⅲ. ①电子商务－支付方式－基本知识 Ⅳ. ①F713.361.3

中国版本图书馆CIP数据核字(2018)第235536号

◆ 著　[英]丹尼尔·德雷舍（Daniel Drescher）
译　马 丹　王扶桑　张初阳
责任编辑　郎静波
责任印制　陈 犇

◆ 人民邮电出版社出版发行　北京市丰台区成寿寺路 11 号
邮编　100164　电子邮件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
三河市君旺印务有限公司印刷

◆ 开本：700×1000　1/16
印张：12.75　2018 年 11 月第 1 版
字数：224 千字　2018 年 11 月河北第 1 次印刷
著作权合同登记号　图字：01-2018-3259 号

定价：59.00 元

读者服务热线：(010)81055410　印装质量热线：(010)81055316
反盗版热线：(010)81055315
广告经营许可证：京东工商广登字 20170147 号

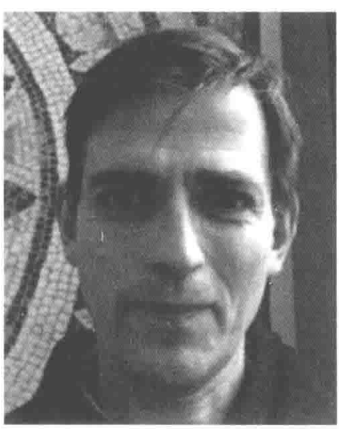
内容提要

通过本书25个简明的章节，读者将学习到区块链的基础知识。全书尽可能避免使用数学公式、程序代码和计算机科学术语，读者无需计算机科学、数学、程序设计和密码学方面的知识也可轻松读懂全书。这本书弥合了关于区块链的纯技术类书籍和纯商业类书籍之间存在的空白，通过解释构成区块链的基础技术概念以及这一技术在相关业务领域中的应用来让读者真正了解区块链。

本书适合程序员、金融从业人员以及对区块链技术感兴趣的读者阅读。

作者简介

丹尼尔·德雷舍（Daniel Drescher）是一位非常有经验的银行家，曾在多家银行的电子证券交易部门任职。他最近重点研究证券交易领域中自动化、机器学习和大数据技术的应用。除此之外，丹尼尔还拥有柏林工业大学计量经济学博士学位、牛津大学软件工程硕士学位。



审稿人简介

劳伦斯·科克（Laurence Kirk）目前醉心于对分布式账本技术的研究，此前他通过为伦敦市的金融公司撰写低延迟金融应用程序，已获得职业生涯的巨大成功。此后，他到牛津大学开始硕士课程的学习，并且创办了一家与初创企业共同在以太坊平台上开发应用程序的咨询公司。对分布式账本技术的热情，让他现在成了一位以太坊开发者和推广者。

前　言

在前言中，作者会回答一些最重要的问题：为什么每个人都要看这本书？说得更具体些，为什么每个人都需要看这本关于区块链的书？通过阅读前言，你会知道写本书的原因、能从中获得哪些知识以及本书的大致章节结构。

为什么又是一本关于区块链的书？

区块链获得了公众和媒体的大量关注，一些极客宣称区块链是自互联网诞生以来最伟大的发明。因此，在过去几年中，已有大量关于区块链的书籍出版。但是，当想要学习更多区块链的知识时，你会发现自己很容易就迷失在知识的海洋中，这些书有的快速掠过技术细节，有的在很深的层面讨论重要的技术内容。前者没有仔细解释技术细节，不能使读者充分理解区块链；后者假设读者已经拥有了丰富的区块链基础知识，这两者都无法使人满意。

前一类书是纯粹讨论区块链底层技术的，后一类则更像是经管类书籍，主要关心具体的区块链应用和其对经济的影响。本书填补了这两类书籍中间的空白。

理解区块链技术的基础概念对于理解其具体应用、评估初创企业的业务前景和参与区块链对未来经济影响的讨论是十分必要的。没有对重要概念的理解，便无法评估区块链总体的价值和影响力，也无法理解具体区块链应用的价值。本书聚焦在区块链涉及的重要概念上，因为若缺乏对技术概念的理解，将削弱对新技术的深刻认识，也将因不切实际的期待而感到失望。

本书以通俗易懂的形式介绍了区块链的概念，努力做到简明、全面，书中阐述了介绍新技术时一定会被问到的三大问题：这项新技术是什么，为什么我们需要它，它将如何改变我们的生活。

你无法从这本书里获得的知识

本书刻意忽略了与区块链应用相关的内容，侧重于对区块链技术的介绍和解释，不会聚焦在具体的区块链应用案例上，因此，本书不包括以下内容。

- 关于比特币和其他“加密货币”的介绍。
- 关于具体区块链应用的介绍。
- 关于区块链数学证明的内容。

- 关于区块链编程的内容。
- 与区块链相关的法律条款。

但是，在读过本书后，你会在一定程度上获得对以上问题的理解。

你可以从本书中获得的知识

本书解释了区块链相关的一些基础概念，比如交易、哈希值、非对称加密、数据结构、点对点系统、系统完备性和分布式共识算法，并将基于以下 4 个前提对这些概念进行解释。

- 对话的形式。
- 不涉及数学证明，也没有公式。
- 逐步深入。
- 使用类比的介绍方法。

对话的形式

为了易于读者阅读理解，本书刻意用对话的形式写作，且不使用数学和计算机术语。但是，本书介绍和解释了一些参加区块链讨论和理解其他区块链出版物时必要的术语。

不涉及数学证明，也没有公式

区块链的主要组成部分，比如共识机制和挖矿算法，都是基于复杂的数学公式建立起来的，这也是区块链技术的难点所在。但是，为了去除任何不必要的复杂性，避免给读者带来阅读困难，本书将不使用数学符号和公式。

逐步深入

书里各讲的内容构成了理解区块链的基础知识框架，每一讲都精心设计，涵盖了软件工程的基础内容，解释了相关术语，同时指出我们需要区块链的原因，也解释了组成区块链的独立概念之间的关系。本书各讲相互独立且逐渐深入，它们组成了一个理解区块链的完整知识体系。

使用类比的介绍方法

每一讲会介绍一个新概念，所有新概念都参考现实生活中的实例，使用形象化的方式进行讲解。这些类比能够达到 4 个主要目的：第一，它们可为读者接触一个

全新的技术概念做好准备；第二，将技术概念与易于理解的现实生活实例联系在一起，减少读者探究新领域的困难；第三，类比是学习新概念的理想方式；第四，类比的形式可让记忆新概念更加容易。

本书是如何组织的

本书包含五大部分的内容，共分 25 讲，给出了区块链学习的基础知识框架。这些章节涵盖了软件工程的基础内容，解释了相关术语，指出我们需要区块链的原因，也解释了组成区块链的独立概念之间的关系，还涉及区块链应用和相关领域内的一些研究成果。

第 1 部分　区块链术语与技术基础

第 1 讲到第 3 讲解释了与区块链相关的主要概念，以及后续内容中需要掌握的其他概念。第 3 讲结束时，你将对区块链的整个底层概念有一个总体的认知，并且能从更宏观的角度看待区块链。

第 2 部分　为什么这个世界需要区块链

第 4 讲到第 7 讲主要解释为什么需要区块链，它解决了什么问题，为什么要解决这些问题，以及区块链的潜在价值是什么。第 7 讲结束时，你将了解区块链能够解决的问题有哪些，它在哪些领域最具应用价值，以及为什么我们需要它。

第 3 部分　区块链如何工作

第 3 部分是本书的核心，解释了区块链的工作原理。第 8 讲到第 21 讲介绍了与区块链相关的 15 个技术概念。第 21 讲结束时，你将理解区块链的主要概念，以及它们之间是如何相互协作的。

第 4 部分　区块链的局限以及如何克服这些局限

第 22 讲到第 23 讲将聚焦于区块链的局限性，以及造成这些局限的原因，并提出一些可能克服这些局限性的方法。第 23 讲结束时，你将理解最初的区块链应用为什么不适用于更大规模的商业活动，为了克服这些局限需做哪些改进，以及这些改进如何提升区块链的性能。

第 5 部分　如何使用区块链，区块链技术的总结及展望

第 24 讲和第 25 讲介绍了如何在现实生活中使用区块链，如何选择区块链应用，以及区块链技术能够解决什么问题。这一部分还包括了区块链领域目前的热门研究方向和未来发展趋势等内容。第 25 讲结束时，你将对区块链有全面的理解，还将为阅读相关技术文章做好准备，并会成为未来区块链讨论中的积极参与者。

目　录

第1部分
区块链术语与技术基础

这一部分介绍了软件系统的主要概念，并建立了一整套术语体系。另外，还介绍了软件架构的概念，并解释了其与区块链之间的联系。通过本部分最后一讲的内容，你将可认识到区块链存在的意义及其潜力。

第 1 讲
理解分层的概念

从分层与架构的角度了解软件系统

这是本书的第 1 讲，它将是我们后续了解和学习区块链的基础。我会通过这一讲介绍本书中对技术概念的阐释规范。这一讲中你将学习如何分析一个软件系统，以及认识到将软件看作分层集合来分析的重要性。另外，你将了解通过分析一个软件系统中的不同分层能获得什么，以及这种分析方式如何帮助我们理解区块链。最后，我会简要介绍软件系统完备性的概念，并强调其重要性。

隐喻

你有手机吗？我相信回答是“有”，而且很多人还不止一个。那么你对使用手机收发数据的过程中用到的各类无线网络协议了解多少？你对移动通信的基础——电磁波的了解又有多少？

我们中的大多数人对这些问题的细节知之甚少，因为使用手机并不需要你知道这些，并且大多数人都没有时间去学习这些知识。我们在主观上将手机分成两部分，一部分我们需要知道，另一部分我们想当然地选择了忽视。

这种对待技术的态度并不只出现在对待手机上。我们会用同样的态度去对待电视机、计算机以及洗衣机等产品。而因为每个人的经历不同，使用相关产品的目标和体验也就不同，这种主观上的区分是高度个体化且独立的，因此，我和你对手机的主观划分或多或少都有所不同。当我尝试向你解释对于一台手机你需要了解什么、不需要了解什么的时候，这种差别在沟通中会更为显而易见。所以，当学习和讨论新技术时，我们首先需要对技术系统进行统一的划分。

本讲会介绍如何对一个软件系统进行划分，并建立我们接下来对区块链进行学习讨论的基础。

软件系统的分层

在本书中，我们使用两种方法来对软件系统进行分割。

- 应用层与实现层。
- 功能性与非功能性。

应用层与实现层

主观上对系统按照用户需求和内在技术原理进行划分，其实是在区分应用层与实现层。应用层中的所有内容都是从用户需求出发的（比如想要听音乐，想要拍照片，想要订酒店）。实现层中的一切都是使得这些需求落地实现的内容（比如，将电信号转变成模拟信号，在数码相机中识别一个像素的颜色，或者将信息通过互联网传给一个预设的系统）。实现层中的所有内容本质上都是技术性的，并且都会被当作达到目标的方法。

功能性与非功能性

考虑一个系统能够做什么和这个系统做得怎么样是有区别的，这就是对系统做功能性和非功能性划分的基础。

功能性特征的例子包括通过网络发送数据、播放音乐、拍摄照片和修改图片中一个特定的像素。非功能性特征的例子包括一个好看的可视化用户界面，快速运行的软件，以及安全、私密地保存用户数据的能力。对于一个软件系统而言，安全性与完备性这两类非功能性特征非常重要。完备性指的是如何设计系统的运行规则，

并让系统具备诸如安全性和正确性等很多特征。我们可以通过英语中对语法的使用来帮助你理解功能性和非功能性特征之间的区别：动词描述了动作或已经完成的行为，而副词描述了一个动作是如何被完成的。举个例子，一个人能够快步走或慢步走。无论快慢，走这个动作是一样的，而这个动作的表现是有区别的。按照这样的理解，你可以认为功能性特征和动词相似，而非功能性特征和副词相似。

同时使用两种划分标准

对于一个软件系统，我们可以在识别其技术性特征与非技术性特征的同时识别应用层与实现层。表 1-1 是一个对手机同时使用两种划分方法的示例。

表1-1 对手机同时使用两种划分方法的示例

分层	功能性特征	非功能性特征
应用层	拍照片	拥有漂亮的用户界面
	打电话	操作简单
	发邮件	拍出的照片效果很好
	上网	
	玩游戏	
实现层	永久保存本地数据	高效存储数据
	自动连接最近的基站	省电
	使用硬件加速优化屏幕的动画效果	确保用户隐私的安全性

表 1-1 可以解释一个系统中不同组成部分对用户的主观可见性。应用层的功能性特征是系统中最抢眼的部分，因为它们满足了用户的明确需求，这些部分一般来说就是用户愿意学习并深入了解的。另一方面，实现层的非功能性特征很少会被视作系统的主要组成部分，而且它们往往会被人们忽视掉。

完备性

完备性在任何软件系统中都是重要的非功能性特征，它往往包含以下 3 个方面的内容。

- 数据完备性：软件系统中的数据要完整、正确且无冲突。
- 行为完备性：软件系统要可顺利运行，并且保证不存在逻辑错误。
- 安全性：软件系统只对认证用户授权有限的数据访问与使用功能。

很重要的一点是，几乎每个人都认为任何一个软件系统都应该具有如上所述的完备性，而忽略了在软件系统背后付出巨大时间和精力的软件工程师，并且只有在软件系统出现各类问题时，才会意识到完备性的重要性。因此，当意识到软件工程师们为了高度完备性所做出的努力时，我们会有种被宠坏的感觉。但是当使用的系统出现问题时，我们的感觉就完全不同了。当你遇到数据丢失，或发现陌生人可以访问你的数据时，你会感觉非常不好。而当手机、计算机、电子邮箱、Word 或 Execl 出问题让你感到生气时，你会忘记自己的好脾气！在这些情景中，我们开始意识到软件完备性是多么重要。因此，我们就不需要诧异为什么如此多的专家会把大量的时间和努力花费在实现层中这些看着不起眼的非功能性特征上了。

下一讲展望

本讲对软件工程的基础知识进行了介绍，其中我们重点学习了软件系统的完备性、功能性特征与非功能性特征，以及应用层与实现层的划分等知识。理解这些概念会帮助你意识到区块链所处的巨大舞台。下一讲我们会使用本讲中介绍的概念去对区块链系统进行分析。

本讲小结

- 软件系统可以通过如下划分来进一步进行分析。
  - ▶ 应用层与实现层。
  - ▶ 功能性特征与非功能性特征。
- 应用层关注用户的需求，实现层则关注如何满足这些需求。
- 功能性特征关注实现了什么，非功能性特征关注这些东西实现得怎么样。
- 大多数用户关注软件系统应用层的功能性特征，而很少关注其中的非功能性特征，特别是实现层的非功能性特征。
- 对于任何软件系统而言，完备性都是一个很重要的非功能性特征，它包括有3个方面的内容：
  - ▶ 数据完备性。

- 行为完备性。
- 安全性。

- 大多数软件错误，比如数据丢失，或被陌生人访问了用户数据，都是系统缺乏完备性导致的。

第 2 讲
纵观全局

区块链与软件架构

本讲将描绘区块链技术所处软件系统的大环境，同时也将重点指出区块链在该大环境中的位置。首先，为了让你理解这一大环境，我会介绍软件架构的概念，并解释软件架构与系统分层之间的联系。然后，为了介绍区块链在大环境中的位置，我们会详细解释区块链与不同软件架构的关系。最后，我们会用一句话讲明白区块链的核心作用。理解区块链的作用是成功理解区块链的基础，也是我们接下来所介绍内容的基础。

隐喻

你买过车吗？即使没有买过车，你大概也知道一辆车可以配置不同的发动机（依靠油、天然气或者电来驱动）。如果我们对汽车进行分层拆分，可以将汽车的发动机看作一个模块。选配不同类型的发动机会给汽车带来巨大的差别，两辆外观相同的汽车会因为配置了不同的发动机而带来极为不同的驾驶体验。同时你对汽车发动机的选择会显著影响汽车的售价、保养开销、所用燃料、排气系统以及刹车系统。